

REMARKS

Reconsideration and allowance are respectfully requested in view of the following remarks. Claims 1-13 are pending in the present application.

Claim Objections

Claims 3, 6, 10 and 11 are objected to for alleged informalities.

The Examiner refers to "MPEP Rule 1.96", i.e., 37 C.F.R. §1.96. This rule provides that "[i]f the computer program listing is contained in 300 lines or fewer, with each line of 72 characters or fewer, it may be submitted either as drawings or as part of the specification." It is respectfully submitted that the specification complies with this requirement. See, for example, pages 4-7, 10-13, 15 and 18 of the present application.

37 C.F.R. §1.96 is not directed to formalities in claims. Applicants submit that it is not clear how the Examiner applies 37 C.F.R. §1.96 to claims 3, 6, 10 and 11. Further, it is not clear what informalities are present in claims 3, 6, 10 and 11.

Applicants request that the Examiner withdraw the objection to claims 3, 6, 10 and 11. If the Examiner maintains such objection, Applicants request that the Examiner explain the specific basis for the objection.

Claims Rejections 35 U.S.C. § 112

Claims 3, 6, 10, and 11 are rejected under 35 U.S.C. 112, second paragraph. The Examiner asserts that claims 3, 6, 10 and 11 merely describe "programmatic" steps, and that "[c]laims 3, 6, 10 and 11 cannot be construed by one of ordinary skill

in the art to distinctly point out definitive claim limitations." The basis for this assertion is not understood.

Applicants submit that claims 3, 6, 10 and 11 recite distinct steps performed in a processor. Each step can be considered as a claim limitation. The claim recites the variables to be loaded, the values assigned to those variables, and the operation performed on each. One of ordinary skill in the art can readily comprehend whether a given method or device performs each of the operations, and therefore falls inside or outside the scope of the claim.

Accordingly, the scope of claims 3, 6, 10 and 11 is clearly defined. Applicants request that the Examiner withdraw the rejection of claims 3, 6, 10 and 11, under 35 U.S.C. 112, second paragraph. If the Examiner maintains such rejection, Applicants request that the Examiner explain why he considers the steps performed in a processor as recited in claims 3, 6, 10 and 11 as failing to distinctly point out claim limitations.

Claim Rejections Under 35 U.S.C. § 103

Claims 1-13 are rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Menezes ("Handbook of Applied Cryptography") in view of Drexler et al. (U.S. Patent Application Publication No. 2003/0061498, hereinafter "Drexler"). This rejection is traversed as follows.

A method including iterations is sensitive to covert channel attacks if at each iteration of the method, the number of operations performed during the iteration varies according to the result bit obtained during the iteration.

According to Applicants' exemplary embodiments, an integer division is performed during a cryptographic method with the same number and type of operations at each iteration, regardless the value of the bit obtained, so that the method is secured against covert channel attacks. For example, according to Applicants' exemplary embodiments, an integer division can be performed with the following steps:

For $j = 1$ to $(m-n+1)$, do:

$a \leftarrow \text{SHL}_{m+1}(a, 1) ; \sigma \leftarrow \text{carry}$

$A \leftarrow (\sigma')\text{SUB}_n(A, b) + (\neg\sigma')\text{ADD}_n(A, b)$

$\sigma \leftarrow (\sigma' \text{ AND } \sigma) / (\sigma' \text{ AND } \text{carry}) / (\sigma' \text{ AND } \text{carry})$

$\text{lsb}(a) \sigma'$

$\sigma' \leftarrow \sigma$

End For

In the above example, during each iteration of the "For Loop," the number of operations performed is the same. It is not dependent upon the results that are produced.

In contrast, Menezes discloses a multiple-precision division method that includes a "While Loop" in each iteration of the "For Loop." Specifically, Menezes discloses the following steps:

3. For i from n down to $(t + 1)$ do the following:

3.1 If $x_i = y_t$ then set $q_{i-t-1} \leftarrow b - 1$; otherwise set $q_{i-t-1} \leftarrow \lfloor (x_i b + x_{i-1}) / y_t \rfloor$.

3.2 While $(q_{i-t-1}(y_t b + y_{t-1}) > x_i b^2 + x_{i-1} b + x_{i-2})$ do: $q_{i-t-1} \leftarrow q_{i-t-1} - 1$.

3.3 $x \leftarrow x - q_{i-t-1} y b^{i-t-1}$.

3.4 If $x < 0$ then set $x \leftarrow x + y b^{i-t-1}$ and $q_{i-t-1} \leftarrow q_{i-t-1} - 1$.

According to Menezes, in step 3.2, the operation in the "While Loop"

repeatedly executes until the expression in the While condition no longer holds true. For each iteration of the "For Loop," the values in the expression of the While condition are different, and thus, the number of operations performed is different. For example, the operation in the "While Loop" might execute twice for the first iteration of the "For Loop," and five times for the second iteration of the "For Loop."

As such, the method in Menezes is sensitive to covert channel attacks because at each iteration of the method, the number of operations performed during the iteration varies according to the result bit obtained during the iteration. In contrast, claim 1 recites repeating step (i) for $m-n+1$ iterations with the same number and type of operations being performed at each iteration, regardless of the value of the quotient bit obtained, to obtain the quotient q . Accordingly, Menezes fails to disclose the above-recited features of claim 1.

In response to Applicants' arguments in the October 23, 2009 Amendment, the Examiner asserts that according to Menezes, the way in which the integer division process is carried out will not change until the condition of the "For Loop" is met.

Applicants submit that even assuming the Examiner is correct with such characterization of Menezes, the reference, at most, discloses an integer division process using iterative steps of a "For Loop." It is not clear what the Examiner means by the "way" in which the process is carried out. Regardless of the intended meaning, however, what is important is that Menezes fails to disclose that the same number and type of operations are performed at each iteration of the "For Loop." As such, it does not meet the recitations of the claim.

Drexler, relied upon for allegedly disclosing that at least one of the numbers a and b comprises secret data, and generating encrypted and decrypted data in accordance with said quotient, does not remedy the above-noted deficiencies of Menezes.

In view of the foregoing, claim 1 is patentable. Claims 2-13 are patentable at least because of their dependency from claim 1.

CONCLUSION


From the foregoing, further and favorable action in the form of a Notice of Allowance is respectfully requested and such action is earnestly solicited.

In the event that there are any questions concerning this amendment, or the application in general, the Examiner is respectfully requested to telephone the undersigned so that prosecution of present application may be expedited.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: April 26, 2010

By: 
James A. LaBarre
Registration No. 32858

Customer No. 21839
703 836 6620